

## ACCOUNT ADMINISTRATOR

The ACES User Account Maintenance function is designed so your agency can maintain your own ACES user accounts. The designated Account Administrator will grant access to employees within your organization.

### Account Administrator Roles and Responsibilities

The Account Administrator performs the following maintenance activities for your agency's user accounts by:

- Creating new user accounts
- Modifying existing user accounts (adding or deleting ACES functions and/or changing user demographic information)
- Performing Password Maintenance (disabling, unlocking and resetting passwords for user accounts within your agency)
- Maintaining user contact information, such as:
  - Phone
  - Fax
  - E-mail address

In order to maintain information security and comply with the CalPERS ACES Security Agreement, it is the ACES Account Administrator's responsibility to:

- Have a signed [Employer User Security Agreement](#) (PERS-AESD-43) form on file for each employee with ACES access
- Maintain all signed *Employer User Security Agreement* (PERS-AESD-43) forms on file for the life of the agreement PLUS two (2) years after the agreement has ended to ensure ACES security compliance
- Immediately disable the ACES access of any employee no longer needing access, leaving employment, or taking an extended leave of absence
- Fill out online and electronically send the [Delete "ACES User Access"](#) (PERS-AESD-42) form to CalPERS using the "Submit" button. After using the "Submit" button, the form will be sent directly to the ACES e-mail box. Please do NOT fax a duplicate copy of the form to CalPERS. (However, if the CalPERS Web page or e-mail is not working, you may use a hard copy of the form, found on page 123 of this User Guide, manually fill it out, and fax it to ACES at 916-795-1523.)
- Maintain a copy of the [Delete "ACES User Access"](#) form (PERS-AESD-42) on file for two (2) years after the user has been deleted from your agency's ACES User List

**NOTE:** Do not fill out and send the AESD-42 if the employee is on a leave of absence and will resume ACES duties upon their return. When the employee leaves, please disable his/her account; when he/she returns and needs ACES access again, please call **888 CalPERS** (or **888-225-7377**) to have the account re-enabled.

Users should contact their Account Administrator for any issues relating to their user account. If the Account Administrator is unavailable, please call the CalPERS Employer Contact Center at **888 CalPERS** (or **888-225-7377**).

### Security Guidelines

ACES provides a secure environment for transmitting sensitive employee information to CalPERS for processing. Creating a user account and granting an employee access to ACES will allow them to enter an environment with privileged employee information. Guidelines have been created to protect this personal information. The following are guidelines for providing access to ACES:

- CalPERS security documents must be filled out by all employees having access to ACES. You must keep a signed copy of all security documents on file for each Account Administrator and other ACES users at your agency. In the event of a CalPERS security review, you may be requested to provide security documents for all current and former ACES users.
- Signing the security agreements means that you will only grant access to functions that CalPERS has approved or trained your agency to use. For example, if your agency has view-only access (Participant Inquiry or Public Agency Billing), then a user shouldn't be granted Internet Forms if he/she does not process transactions or has not been trained on Internet Forms. If you are unsure of what this security requirement entails, contact the Employer Contact Center at **888 CalPERS** (or **888-225-7377**) or see the ACES & Other Online Services Web page:  
<http://www.calpers.ca.gov/index.jsp?bc=/employer/aces/user-guide-resources/security-forms.xml>.
- The CalPERS Security Policy requires each person to have his or her own ACES account. **Users are not allowed to share user names and passwords.**
- CalPERS encourages your agency to designate more than one Account Administrator. In the event that the primary Account Administrator leaves your organization, changes positions, or is simply on vacation, another individual is able to maintain ACES user accounts.
- When an Account Administrator leaves an agency or no longer requires access to ACES, your agency should immediately disable their ACES account and submit a [Delete "ACES User Access"](#) (PERS-AESD-42) form to CalPERS and establish another Account Administrator for your agency.
- If security has been violated or ACES has been misused by a user, the Account Administrator should revoke the user's access to ACES immediately.

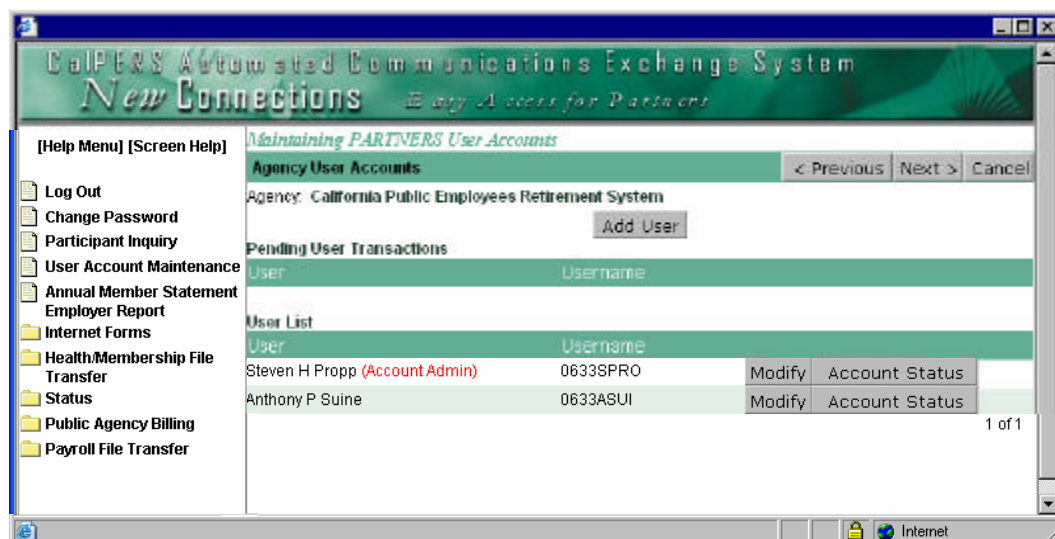
## Logging On to the User Account Maintenance Function

Select **User Account Maintenance** from the Navigation Tree.



## Agency User Accounts

This screen lists the current user accounts at your agency and, if applicable, will display any pending transactions. This screen serves as a “home page” for user account maintenance.



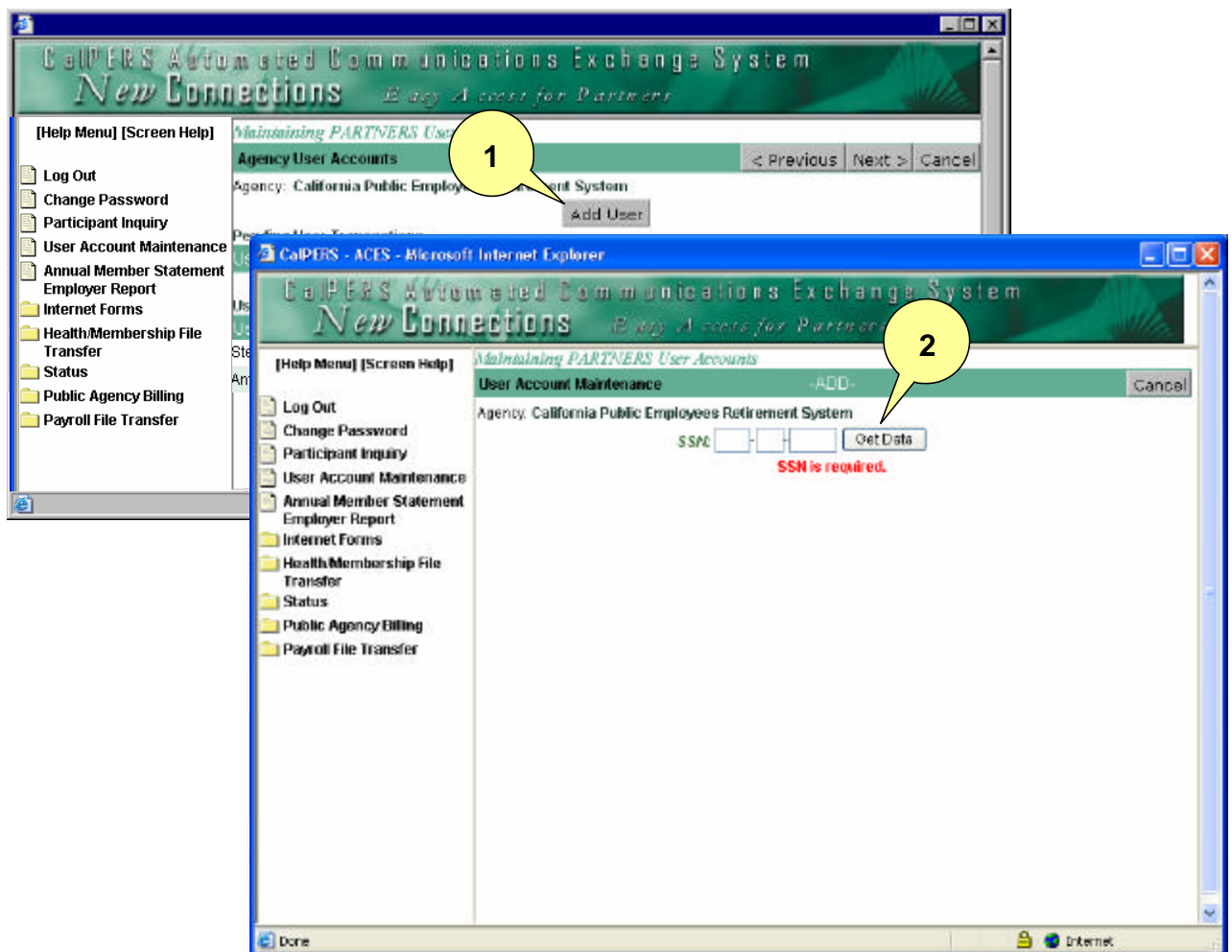
Through the **Agency User Accounts** table you can:

- Add new users
- Modify demographic information (e.g., edit phone number, e-mail address)
- Modify access rights
- Perform password maintenance (unlock accounts and reset passwords)
- Disable user accounts

## Adding a New User

Have the employee fill out a security document (located at the end of this section or <http://www.calpers.ca.gov/index.jsp?bc=/employer/aces/user-guide-resources/security-forms.xml>).

1. Select **Add User** from the Agency User Accounts screen.
2. Type the SSN and click **Get Data**.

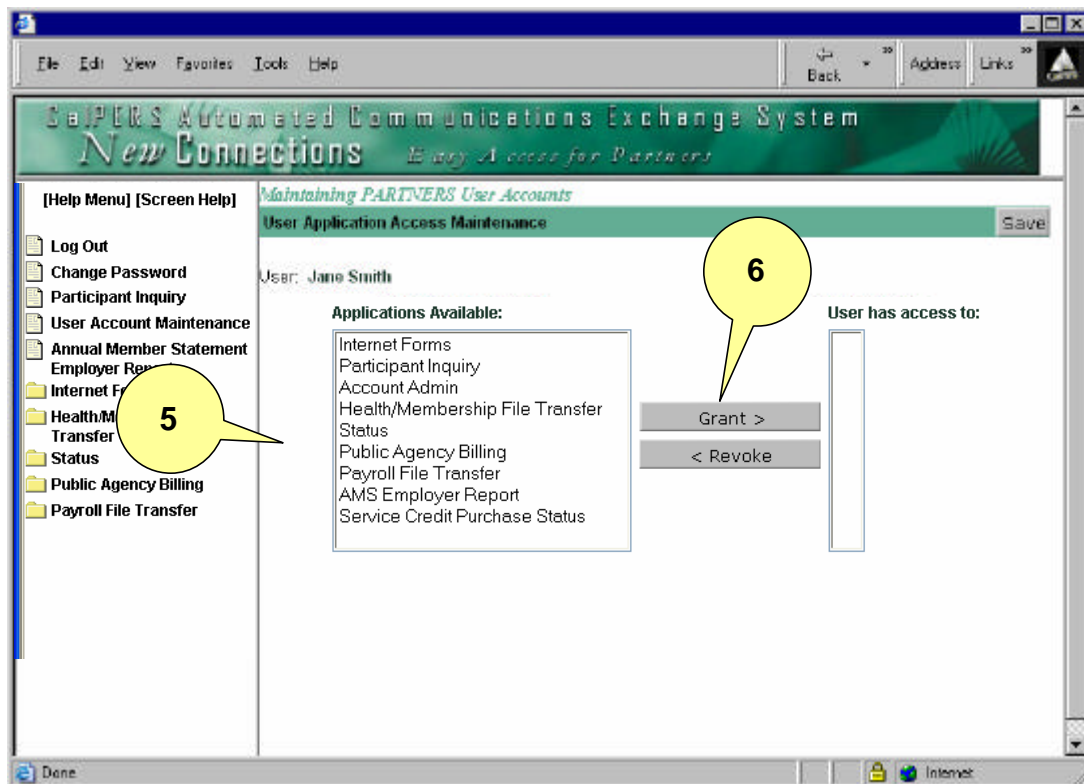


**NOTE:** You might enter an SSN and receive the error message “**SSN XXX-XX-XXXX does not exist in the CalPERS database. Please contact us at 888 CalPERS (or 888-225-7377) for assistance.**” To resolve this error:

- Verify the SSN has been typed correctly
- If you’ve entered the SSN correctly, please fax the security document to CalPERS at 916-795-1523, Attention: ACES. CalPERS will add the new user for you.

3. Enter the demographic information for the user (*green /bold /italic* fields are required):
  - **Phone** (The user's **business** phone number)
  - Fax
  - **E-mail Address**
  - **E-mail Address** (entered a second time for confirmation)
  - Business Mailing Address
4. Click **Save**. A new window will appear.

5. Select an ACES function from the “Applications Available” list at the left of the screen by clicking on the desired function.
  - You may grant multiple functions at once by holding down the “Ctrl” key and clicking on each desired function
6. Once function(s) are highlighted, click **Grant**.

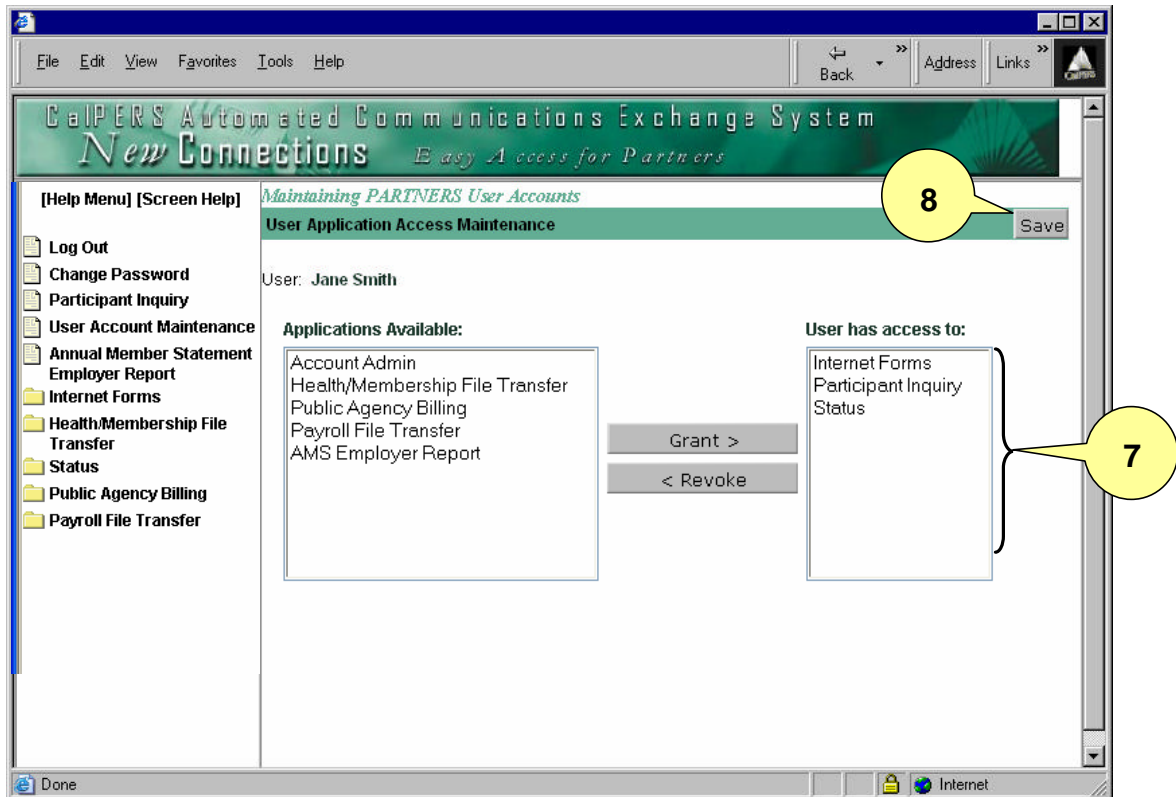


\* **IMPORTANT NOTE:** When granting access to the **Internet Forms**, **Account Administrator**, or **Health/Membership File Transfer** applications, you **MUST** grant the user access to the **Status** application as well

**Note:** Agencies must maintain all signed *Employer User Security Agreement* (PERS-AESD-43) forms on file for the life of the agreement PLUS two (2) years after the agreement has ended to ensure ACES security compliance.



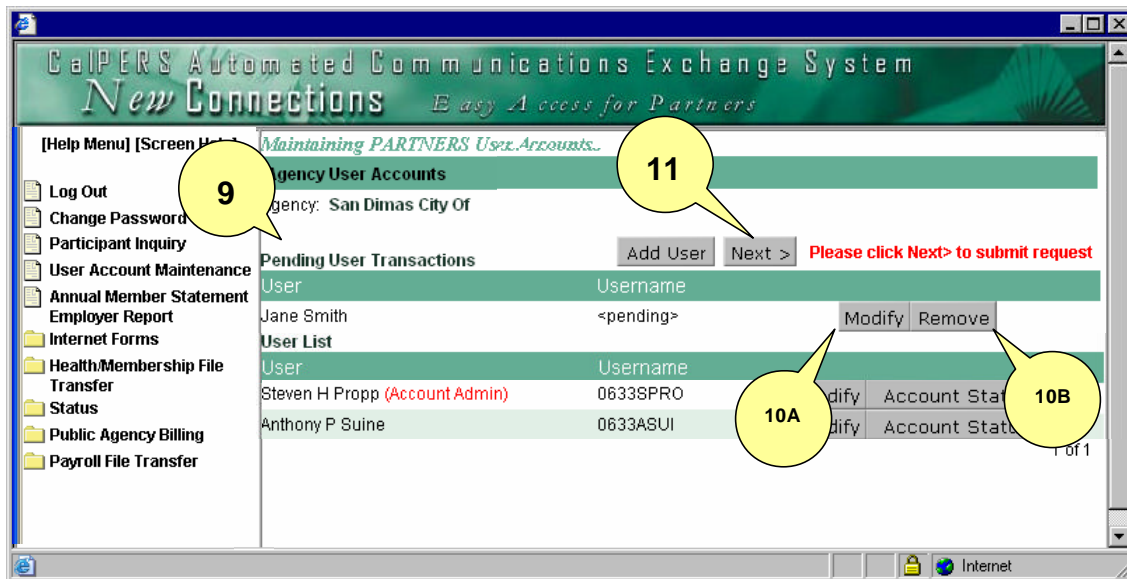
7. The function selected will move to the “User has access to” list.
- REMINDER: You should only grant access to functions for which your agency has been approved and trained. (See Security Guidelines section for more information or contact the Employer Contact Center at **888 CalPERS** [or **888-225-7377**] for more information.)



Repeat Steps 5 and 6 until all appropriate ACES functions have been added for this user.

8. Click **Save**.

9. The new user's name will appear in the "Pending User Transactions" list above the table of current users.
10. To add additional users, repeat Steps 1 through 10.



### Optional:

- A. To change the demographic information or access to ACES functions for a new user, click **Modify**. The existing data for that user will appear. Make the desired changes and click **Save**.
  - B. If you've added a user in error, click **Remove** to delete the user. A dialog box will appear. Click **Ok** to remove the user or **Cancel** to keep the user.
11. When you are done adding users, click **Next** to submit the request to CalPERS.

**Important:** Pending User Transactions will be lost if you click outside of the Agency User Accounts screen before submitting your request to process Pending User Transactions to CalPERS.



12. Type the correct e-mail address where confirmation of your processed request is to be sent.

The top screenshot shows the 'CalPERS Automated Communications Exchange System' interface. The left sidebar contains a menu with options: Log Out, Change Password, Participant Inquiry, User Account Maintenance, Annual Member Statement, Employer Report, Internet Forms, Health/Membership File Transfer, Status, Public Agency Billing, and Payroll File Transfer. The main content area is titled 'Maintaining PARTNERS User Accounts' and includes a 'Verify Updates' section. A callout '12' points to the 'E-Mail Address:' input field. A callout '13' points to the 'Submit Request' button. The bottom screenshot shows the 'Request Status' page. It displays the following information: Agency: San Dimas City Of, Your updates were successfully submitted, Your Tracking ID is: 2473440 (with callout '14'), Your updates will be processed within 24 hours, and You will be notified via E-Mail at: m@m.com. The date and time 'Fri Jan 03 14:59:03 PST 2003' are shown in the top right corner.

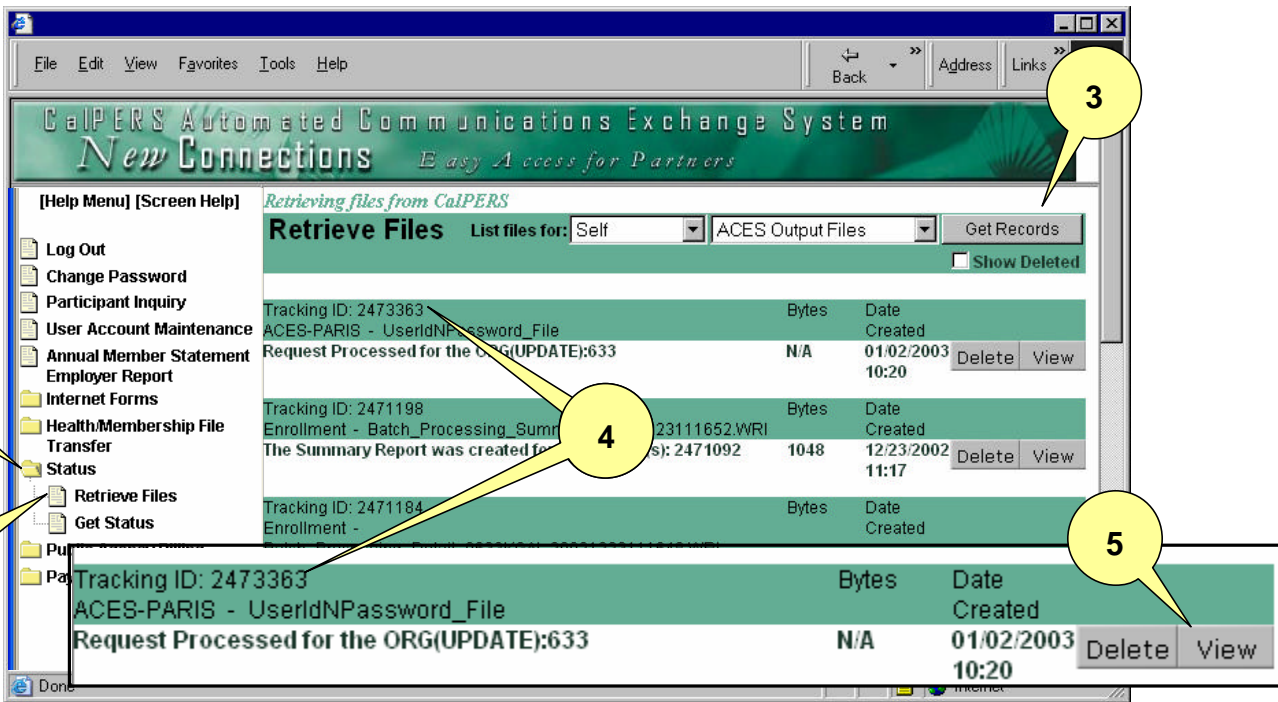
13. Click **Submit Request**.

14. Make note of the Tracking ID number.

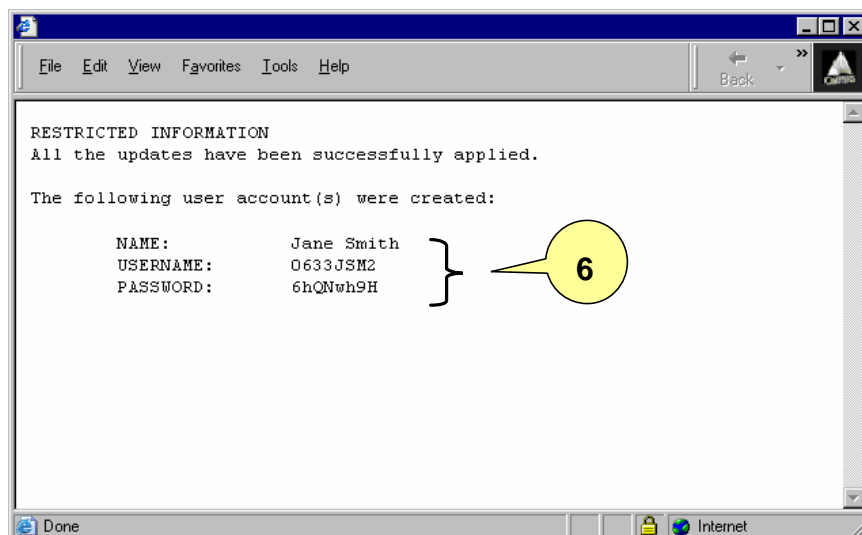
**NOTE:** Requests submitted before 6:00 p.m. are processed the same day. You will receive an e-mail when the username(s) and password(s) are available; however, new users will not have access to the applications of ACES until the following business day.

## Retrieving Passwords for New Users

1. Select the **Status** folder.
2. Select **Retrieve Files**.



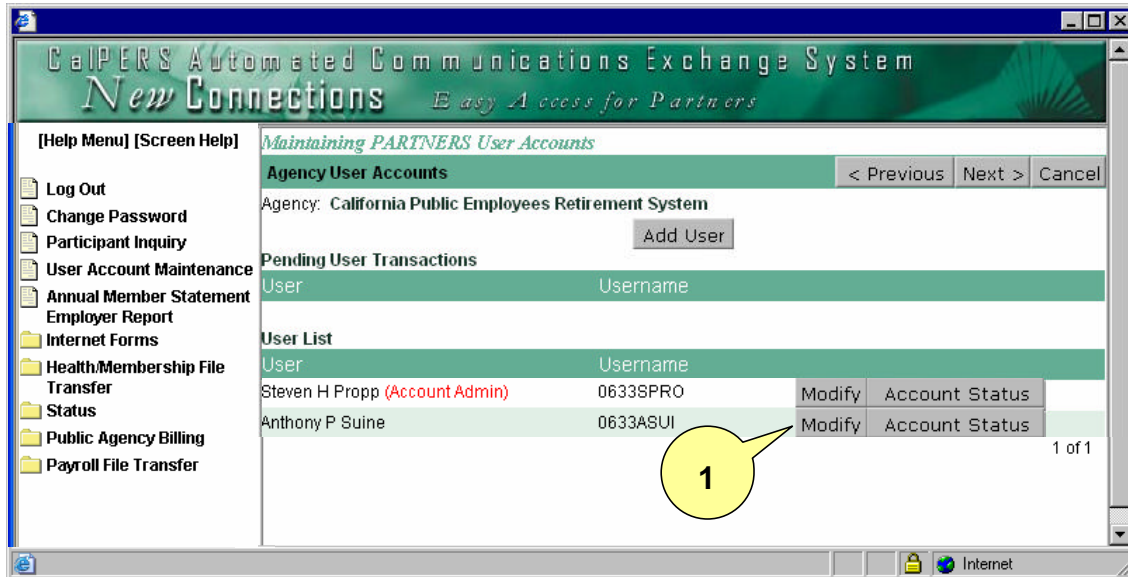
3. Click **Get Records**.
4. Locate the Tracking ID number from your request.
5. Click **View**.
6. The ACES Username(s) and Password(s) will be listed. Forward the username and password to the appropriate user(s).  
**NOTE:** Neither the user name nor the password are case-sensitive.



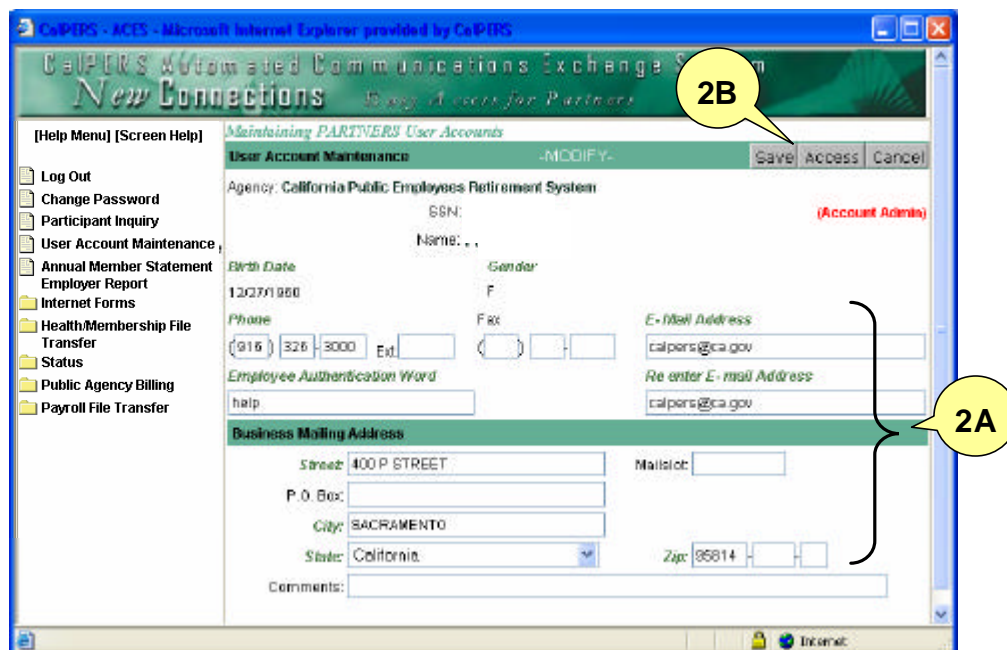
## Modifying User Information

Use the **Modify** button to make changes to a user's demographic information (e.g., address, phone number) and/or change a user's access to ACES functions.

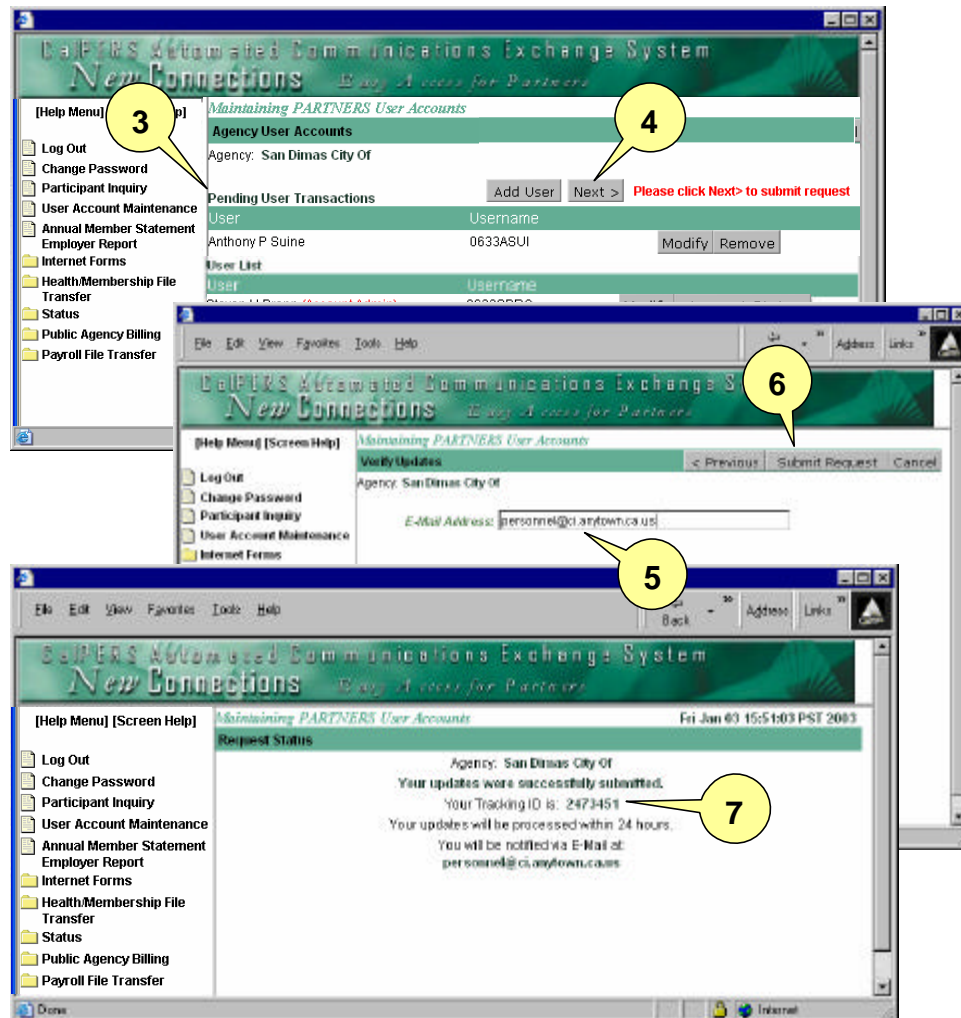
1. Click the **Modify** button from the Agency User Accounts screen.



2. The user's information appears.
  - A. **For Demographic changes:** Make desired changes to the user's existing information. Click **Save** after you've made the appropriate changes. The Agency User Account screen will appear. Go to Step 3.
  - B. **For User Access changes:** Click the **Access** button from the Modify screen. The access screen will appear. Highlight the desired function to **Grant** or **Revoke** access (See Pages 113-114, Steps 5-9 for further details).



3. The modified user's name will appear in the "Pending User Transactions" list above the table of current users.
  - To modify additional users, repeat Steps 1 and 2.
4. When you are done modifying users, click **Next**.



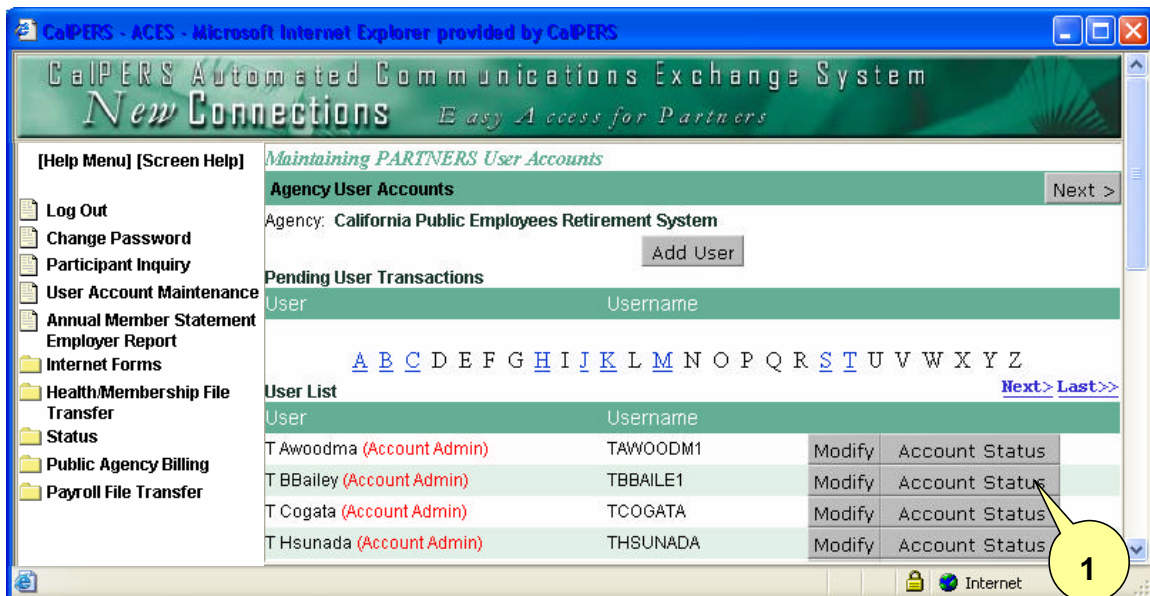
5. Verify your e-mail address.
6. Click on **Submit Request**.
7. Receive Tracking ID number.
  - On modifications, it is not necessary to retrieve a report from Status, Retrieve Files.

**NOTE:** Requests submitted before 6:00 p.m. are processed the same day. You will receive an e-mail when the modifications have been processed; however, the modified information or new access rights will not be reflected in ACES until the next business day.

## Account Maintenance

Use the **Account Status** button on the Agency User Accounts screen to:

- Reset a user's password. If a user misplaces or forgets their ACES password, you can reset their password.
- Unlock a user's account. This action can be performed when a user's account is locked after 4 incorrect log on attempts.
- Disable a user's account. When a user no longer requires ACES access, their ACES account must be disabled immediately. If security has been violated, CalPERS should be notified immediately at **888 CalPERS** (or **888-225-7377**).



1. From the **Agency User Accounts** screen, click on the **Account Status** button. A new window will appear.



2. Choose the desired **Action to Perform** on the selected user account:

AccountStatus - Microsoft Internet Explorer provided by CalPERS

Maintaining Passwords

Close

Agency: California Public Employees Retirement System

Username: TBBAILE1

Employee Authentication Word: help

Last four digits of SSN: XXX-XX-1005

Account Status: **ACTIVE**

Action to perform: -Choose Action- Apply

2

3

-Choose Action-  
Reset Password  
Unlock Account  
Disable Account

- **Reset Password:** Resets a user's password. The user will be prompted to change this temporary password when they log onto ACES after the password reset.
- **Unlock Account:** Restores account to "Active" password status
- **Disable Account:** Disables a user from logging in to ACES

3. Click **Apply**.

- If you have reset a password, the password will appear in red as follows:  
NOTE: The password is not case-sensitive.

AccountStatus - Microsoft Internet Explorer provided by CalPERS

Maintaining Passwords

Close

Agency: California Public Employees Retirement System

Username: TBBAILE1

Employee Authentication Word: help

Last four digits of SSN: XXX-XX-1005

Account Status: **ACTIVE**

Action to perform: -Choose Action- Apply

4

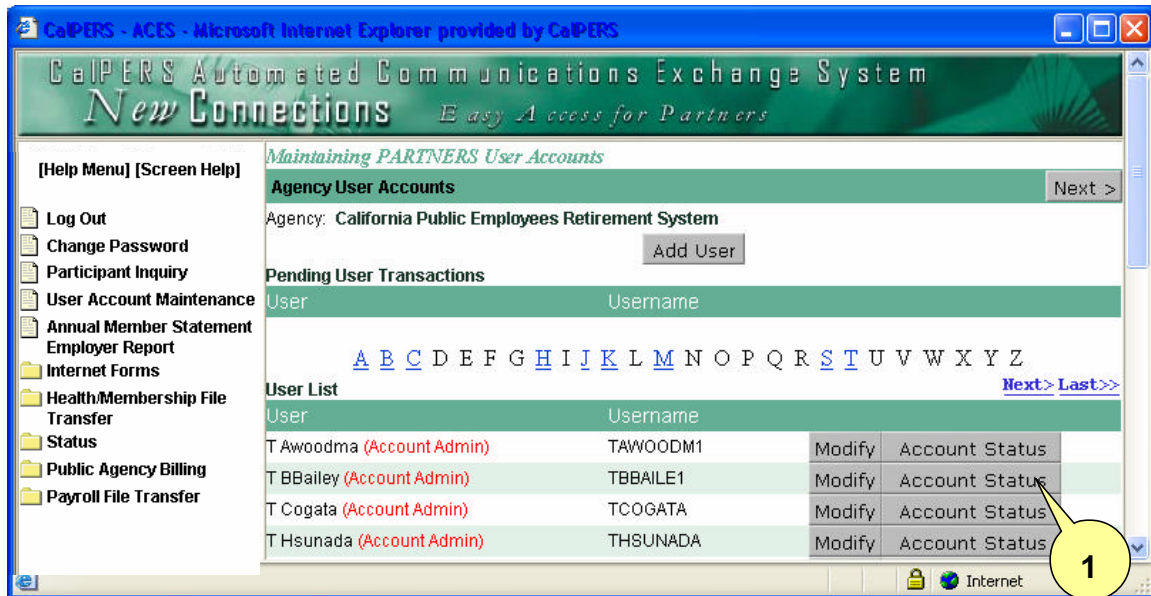
The new password is: **by4hwbcj**

4. Click **Close**.

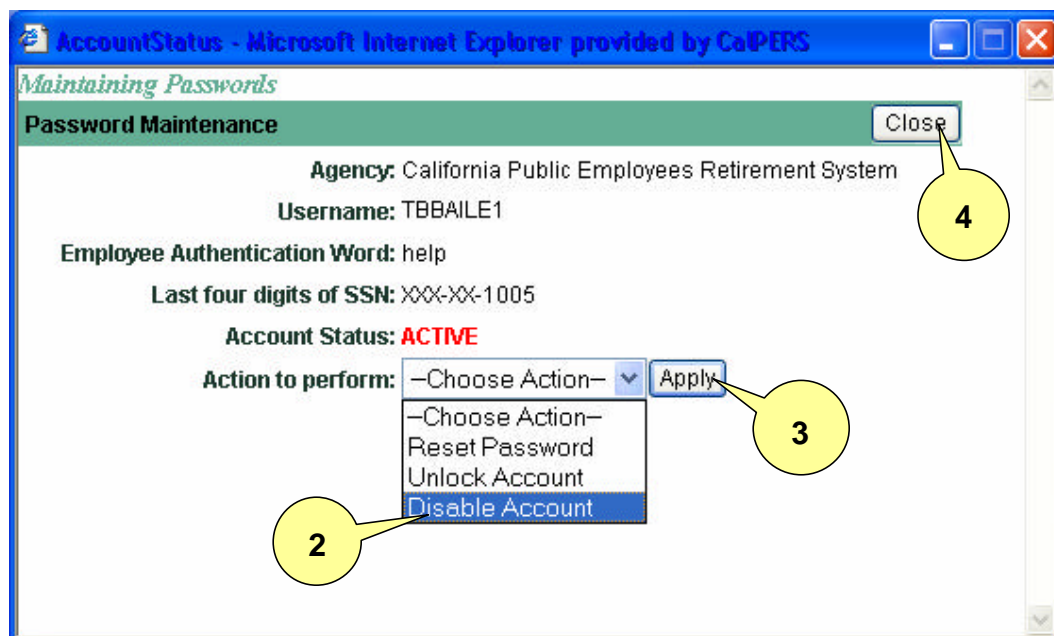


## Disabling and Removing a User

1. A user no longer requiring ACES access **must** be disabled immediately to ensure information security. Click on **Account Status** from the Agency User Accounts page. A new window will open.



2. Click on **Disable Account** in the drop-down box.
3. Click **Apply**. A message will appear within moments confirming the account is disabled.



4. Click **Close**.
5. Fill out a **Delete "ACES User Access"** form (located at <http://www.calpers.ca.gov/jasper/ei/aces-aesd-42/aesd-42-form.jsp>) and electronically send it to CalPERS by using the "Submit" button. CalPERS will remove the user from the table of users.

### Password Requirements

When resetting passwords, the system automatically generates a random password. This is a temporary password used to initially log the user into ACES. Upon successfully logging in, the user will be required to change this temporary password to one of their choosing.

The following are the ACES password requirements:

- Your password must be no fewer than 8 and no more than 12 characters long
- Your password must be a combination of alpha and numeric characters
- Your password cannot be the same as your user name
- Please note that if you enter your password incorrectly four times when attempting to log on, you will be locked out of ACES. Contact your agency's Account Administrator to unlock your account. For further assistance, call the Employer Contact Center at **888 CalPERS** (or **888-225-7377**).
- You will be prompted to change your password every 60 days

**NOTE:** If you change your password every 60 days by changing only one digit (e.g., "password1" to "password2" to password3" etc.), the CalPERS system "recycles" passwords after ten (10) changes. This means after reaching "password10" that you may start back at "password1" if you wish.

## CALIFORNIA PUBLIC EMPLOYEES' RETIREMENT SYSTEM EMPLOYER USER SECURITY AGREEMENT

(TO BE COMPLETED BY EMPLOYER AND EMPLOYEE) (PLEASE COMPLETE ONLINE OR PRINT LEGIBLY)

EMPLOYEE		EMPLOYER
Employee Name:		Employer Name:
Employee Social Security Number:	Date of Birth:	Employer Code (CalPERS):
Employee Business Phone:	Employee Business Fax:	Employer Mailing Address:
Employee Business E-mail Address:		Employer Physical Address: (if different than mailing)
<p><i>Please check all that apply:</i></p> <div style="display: flex; flex-wrap: wrap;"> <div style="width: 33%;"><input type="checkbox"/> <b>Account Administrator</b></div> <div style="width: 33%;"><input type="checkbox"/> <b>Internet Forms: Health</b></div> <div style="width: 33%;"><input type="checkbox"/> <b>Internet Forms: Membership</b></div> <div style="width: 33%;"><input type="checkbox"/> <b>Public Agency Billing</b></div> <div style="width: 33%;"><input type="checkbox"/> <b>Annual Member Statement Employer Report</b></div> <div style="width: 33%;"><input type="checkbox"/> <b>Service Credit Purchase Status</b></div> <div style="width: 33%;"><input type="checkbox"/> <b>Participant Inquiry</b></div> <div style="width: 33%;"><input type="checkbox"/> <b>Payroll File Transfer</b></div> <div style="width: 33%;"><input type="checkbox"/> <b>Annual Employer Statement</b></div> </div>		

By signing this document, the employee referenced above acknowledges reading, understanding, and agreeing to its contents and realizes the consequences of not complying with the terms stated below.

### ACES User responsibilities:

- Passwords must be kept confidential. Reasonable precaution must be maintained including but not limited to:
  - Not sharing or allowing others access to your password for any reason
  - Securing the terminal with a password or locking device when logged onto ACES, when leaving the workstation
  - Immediately reporting any suspicious circumstances or unauthorized individuals observed in the work area to a supervisor
- Access and/or transmit information only relevant and necessary in the ordinary course of performing job official duties
- CalPERS record information shall only be disclosed to individuals when relevant and necessary when performing official duties. Unauthorized disclosures include, but are not limited to:
  - Disclosing social security number of another person when not part of job responsibilities.
- CalPERS record information shall not be transmitted or used for personal reasons, including but not limited to:
  - Making personal inquiries of friends or relatives; accessing information about another person, including locating their residence address, for any reason that is not related to job responsibilities

### ACES Administrators' responsibilities:

- Maintain all **California Public Employees' Retirement System Employer User Security Agreement** forms (AESD-43) and **Delete "ACES User Access"** forms (AESD-42) in a secured location
- Ensure Security Agreements are fully completed and signed by a manager or supervisor prior to processing or faxing to CalPERS. Completed forms may be faxed to 916-795-1523.
- Immediately fill out, electronically submit, and maintain a copy of the **Delete "ACES User Access"** form (AESD-42) for all ACES users who no longer have ACES access for two years
- Direct staff that:
  - Passwords must be kept confidential at all times and not be shared for any reason
  - Computer terminals must be secured with a password or locking device when unattended and logged into ACES
  - Suspicious circumstances and unauthorized individuals should be reported immediately to a manager or supervisor

I have read and understand the security policies stated above. I acknowledge and agree to utilize all CalPERS systems in accordance with the terms outlined in the California Public Employees' Retirement Law and CalPERS business practices, policies, and procedures. Failure to comply with these policies may result in revocation of my access to ACES, adverse action, and/or civil or criminal liability under applicable laws. I further understand that I can undergo disciplinary action from my employer up to and including termination of employment.

I certify under penalty of perjury, under the laws of the State of California, that the information provided above is true and correct.

The California Public Employees' Retirement System (CalPERS) collects personal information to administer the various programs, accessed through the Automated Communications Exchange System (ACES), for which it has responsibility. Employers may NOT share information with any other entity without the express written approval of CalPERS. The information contained in CalPERS records is confidential, and CalPERS is required by law to protect such information from unauthorized access, use, and disclosure.

Employee Signature:	Date:
Employer Signature: (Manager/Supervisor)	Date:

This form must be completed for each employee using CalPERS online access and be available to CalPERS upon request. Forms must be **RETAINED IN A SECURE WORK SITE LOCATION** of the Employer, for the life of the Agreement and for two (2) years following the deactivation or termination of the Agreement. CalPERS is to be notified immediately in the event that any of its sensitive or confidential information is subjected to unauthorized disclosure, modification or destruction. Completed forms may be faxed to 916-795-1523.

Clear

Submit

## Symbol Key

\* Required Field

← Missed Field

## CALIFORNIA PUBLIC EMPLOYEES' RETIREMENT SYSTEM DELETE ACES USER ACCESS FORM

PLEASE COMPLETE ONLINE OR PRINT LEGIBLY

### Section 1. To be completed by employer

* Employee Name: <input style="width: 90%;" type="text"/>	* Employer Name: <input style="width: 90%;" type="text"/> * CalPERS Employer Code: <input style="width: 90%;" type="text"/>
Employee's ACES User Name (e.g. 0001coga): <input style="width: 90%;" type="text"/>	* Date user should be deleted: <input style="width: 90%;" type="text"/>

### Section 2. To be completed by employer

Employer Account Administrator, Manager or Supervisor * Name: <input style="width: 90%;" type="text"/> * Phone: ( <input style="width: 20px;" type="text"/> ) <input style="width: 20px;" type="text"/> - <input style="width: 20px;" type="text"/> X <input style="width: 90%;" type="text"/>	* Date: <input style="width: 90%;" type="text" value="7/27/2007"/>
--	--

### Section 3. To be completed by CalPERS

Date Received: <input style="width: 90%;" type="text" value="7/27/2007"/>	Processed by: <input style="width: 90%;" type="text"/>	Date Processed: <input style="width: 90%;" type="text"/>
--	---	---

Comments:

---



---



---

This form must be completed for each ACES User who no longer needs access to ACES or who has terminated employment from your agency. This form must be **RETAINED BY THE EMPLOYER IN A SECURE WORK SITE LOCATION** for two years following the request to delete ACES User access and be available to CalPERS upon request. CalPERS is to be notified immediately in the event any of its sensitive or confidential information is subjected to unauthorized disclosure, modification or destruction. In lieu of submitting this form electronically, completed forms may also be faxed to (916) 795-1523.

If you have any questions or need to change any information, contact us by e-mail ([aces@calpers.ca.gov](mailto:aces@calpers.ca.gov)) or by calling the Employer Contact Center at **888 CalPERS** (or 888-225-7377).